DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

Memo Issued: July 25, 2008
Control #: MITS- 0708-10
Affected IRM: 10.8.32
Expiration Date: 07/31/2009

MEMORANDUM FOR DISTRIBUTION

FROM: /s/ Karen Freeman
Director, Cybersecurity Policy and Programs

SUBJECT: Interim Guidance – Revised Security Controls for IRS Mainframe System (IBM/RACF)

This interim guidance memorandum is being issued in order to quickly communicate revised security controls, for Planning and Identification of Started Tasks. The revised guidance clarifies the requirements for planning of critical resources for the mainframe environment. The change(s) are hereby effective immediately for IRM 10.8.32, *IBM Mainframe System Security Requirements, Sections 10.8.32.3.2, 10.8.32.5.4.1, and Exhibit 10.8.32-2 Appendix B, dated September 1, 2007.*

These requirements shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. The policy applies to all employees, contractors and vendors of the Service.

1. **Source(s) of Authority**: IRM 10.8.32 is issued under the authority of Treasury Directive (TD) 85-01.

2. **Effect on Other Documents:** This IRM updates IRM 10.8.32, dated September 1, 2007.

3. **Contact:** Please send questions or inquiries related to this guidance, to Janice F. Harrison, Program Manager, Cybersecurity Policy and Procedures Management at (202) 283-6762.

4. **Expiration Date**: This guidance will be incorporated into the IRM 10.8.32 on or before July 29, 2009

Attachment (1)
Interim Guidance - IRM 10.8.32, *IBM Mainframe System Security Requirements*

Distribution
Deputy Commissioner for Operation Support
Chief Information Officer

cc: IMD Coordinator
Office of Servicewide Policy, Directives, & Electronic Research
www.IRS.gov

Attachment (1)

Interim Guidance - IRM 10.8.32, *IBM Mainframe System Security Requirements, Sections 10.8.32.3.2, 10.8.32.5.4.1, and Exhibit 10.8.32-2 Appendix B*

The following change(s) are hereby effective immediately for IRM 10.8.32, *IBM Mainframe System Security Requirements*, *Sections 10.8.32.3.2, 10.8.32.5.4.1 and Exhibit 10.8.32-2, dated September 1, 2007.*

CHANGE(s):

10.8.32.3.2
(XX-XX-XXXX)
Planning

(6) The GSS DAA and application owner(s) shall ensure that critical resources are documented in the SSP and the technical project documentation of the GSS.

10.8.32.5.4.1
(XX-XX-XXXX)
Identification of Started Tasks

e. Business requirements shall determine need for User IDs for Started Tasks. User IDs for Started Tasks shall be assigned the "protected" attribute, so that it will be impossible for any user to log on as that started task ID.

f. User IDs for Started Tasks shall only be assigned a TSO segment, USS segment or password, if required for the execution of the started task. If a password is assigned, use shall be limited to only the personnel assigned for maintenance and use of that started task. Any use of that password will be documented to maintain proper accountability and tracking of the individual(s) using the assigned password.

Exhibit 10.8.32-2
(XX-XX-XXXX)
Appendix B: RACF Planning and Implementation

k. Document access decisions in two matrices: dataset access matrix and general resource access matrix. The access matrices outline the accesses and privileges which are authorized to each group for each critical resource on the system. The critical resources shall be identified and documented by the RACF Security Administrator. The assigned Security Specialist and ISSO shall review the documented critical resources. The DAA/ System owner shall approve the documented critical resources.